IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	09/980,271	Examiner:	Brown, Rueben M.
Filed:	November 30, 2001	Group/Art Unit:	2623
Inventor(s):	Alain Delpuch	Atty. Dkt. No:	5266-09100
Title:	FLEXIBLE INTERFACE FOR SECURE INPUT OF PIN CODE		

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date indicated below.

Rory D. Rankin
Registered Representative

Signature — September 11, 2006 (Date)

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request. This request is being filed with a notice of appeal. The review is requested for the reason(s) stated below.

Applicant is in receipt of the Advisory Action mailed August 28, 2006. Claims 1-11 remain pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks.

Claims 1-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,338,138 (hereinafter "Raduchel"), in view of U.S. Patent No. 6,122,741 (hereinafter "Patterson"). The following clear errors in the Examiner's rejection are noted.

By way of preface, Applicant believes it useful to provide a very brief description of the presently claimed invention. Applicant's presently claimed invention is generally directed to a system and method for authenticating a user in order to run an application. More particularly, the claimed invention addresses requirements for security which are contradictory. For example, in order to run an application, an authentication of the user is needed (e.g., using a PIN). It is desired that such authentication be controlled/presented by the application so that, for example, it may have the look and feel of the

application. However, it is also preferred that the PIN code should not be given to the application for security purpose.

Generally, two types of solutions are presently known for authentication. Both present drawbacks, as they are only capable of fulfilling part of the above requirements. In a first case, the application presents its own user interface for PIN entry, receives input, and queries the underlying system to check if the given PIN is correct. However, this solution does not hide the PIN code from the application. In a second case, the application requests the underlying system to authenticate the viewer. For this, the underlying system, using its own look and feel, prompts the viewer for its PIN, verifies its validity, and then returns information that the viewer is or is not authorized. This solution may be safer, but does not allow integration of the PIN entry with the application look and feel.

The presently claimed invention addresses these problems by having the application control presentation of a PIN interface. The application requests user authentication from a security manager. The security manager receives a user's entry and performs authentication. However, as the application does not receive the entered PIN information, the application has no feedback to provide a user who is inputting a PIN. Therefore, the security manager is configured to provide the application with information concerning key pressing operations of the user – without providing the PIN – so that the application can provide feedback to the user concerning their input. As presently claimed, the application presents crypted information in a PIN entry field corresponding to key pressing operations.

Turning now the claims, claim 1 recites:

> "a system for authenticating a PIN code of a user in an interactive information system in order to run an application, the system comprising:
> an input device for entering a PIN code of a user;
> a security manager configured to:
> receive a request for user authentication from the application;
> compare a received PIN code of the user with a registered PIN code, in response to said request;
> supply information to the application about PIN code entering key-pressing operations by the user, wherein the entered PIN code is not supplied to the application; and
> give authorization to run said application if the PIN code of the user matches the registered PIN code;
> wherein the application is configured to present a PIN entry field, wherein crypted information corresponding to said information about PIN code entering key-pressing operations received from the security manager is displayed in the PIN entry field."

In the above, it is first noted that the security manager is configured to "receive a request for user authentication from the application." The recitation "the application" has antecedent basis in the earlier recited "system for authenticating a PIN code of a user in an interactive information system in order to run an application." Claim 1 also recites authorization is given to run said application. In other words, it is the application that a user seeks to run which provides the request for user authentication to the security manager. In addition to providing the request for user authentication, it is this application which is "configured to present a PIN entry field." These features are in accord with the above discussion which describes the application controlling presentation of the PIN interface.

In the Final Office Action dated April 20, 2006, the examiner suggests Raduchel discloses the features:

> "a security manager configured to:
> receive a request for user authentication from the application;
> compare a received PIN code of the user with a registered PIN code, in response to said request;
> supply information to the application about PIN code entering key-pressing operations by the user, wherein the entered PIN code is not supplied to the application"

In particular, the examiner cites the following disclosure of Raduchel:

> "FIG. 2 depicts a flow chart of the steps performed during login to the local computer depicted in FIG. 1"
>
> "When the local computer is initially started, a small portion of the operating system is loaded (step 202). In this step, the minimum code necessary to run authentication is loaded, including VM 117 as well as the minimum components of the operating system necessary to load and run a web browser; it does not include a command interpreter or file capabilities.
>
> Next, the browser is loaded and run (step 204). As shown in FIG. 3, when running the browser, the user is initially presented with a screen 300 having a login dialog box 302 into which the user can enter their username and password. This screen is displayed by an applet, stored with the browser, that performs authentication by communicating with the authentication manager. . . . the authentication information, including the username and password, is sent by the browser to the authentication manager
> . . .
> The authentication manager receives the log-in information and uses it to authenticate the user . . . and returns a token that identifies the services that the user may use (step 406). Additionally, this token may contain a profile of the user's access rights, and when the token is returned to the local computer, it would be included in all further requests from the local computer.
>
> Returning to FIG. 2, the local computer receives the authentication results from the authentication manager and determines if the user was authenticated (step 208). If authentication fails . . . the user is allowed only to perform actions considered non-invasive, such as sending and receiving e-mail, viewing publicly available, non-proprietary web pages via the browser, or viewing on-line calendars. However, if authentication is successful, the user may use all of the available services of the local computer. . . .
>
> If authentication fails, the browser provides the user with restricted access to the local computer (step 210). In this step, the browser displays icons representative of the services that the user may use, as indicated in the token received from the authentication manager. For example, FIG. 5 depicts the browser screen 300 with three icons: icon 502, allowing the user to access an e-mail system; icon 504, allowing the user to use a time management program; and icon 506, allowing the user to browse various web pages on the Internet. Upon selecting one of the icons 502-506 for the first time, the browser sends a request to the authentication manager for the appropriate service applet, and the

> authentication manager downloads it to the browser so that the user may use the corresponding service. Subsequent selections of the icon do not cause a download of the service applet; instead, recognizing that a copy has already been downloaded, the browser merely invokes that copy." (Raduchel, col. 4, line 58 – col. 5, line 62).

The examiner states (page 3 of Final Office Action) that the claimed "application" is "broad enough to read on the browser or any of the services that the user seeks to access." However, Applicant disagrees.

First, as a general matter, it can be seen that Raduchel merely discloses a computer log-on procedure which returns a token that identifies the services that the user may use. The web browser may then display an icon for the services the user has permission to use (i.e., has already be authenticated to use).

Second, it is noted that claim 1 recites "the application is configured to present a PIN entry field." This clearly eliminates the services/icons of Raduchel as being equivalent to the application. Only the *browser* of Raduchel is disclosed as presenting a "login dialog box". Further, the services that are approved have in fact already been approved. Accordingly, should a user select one of the service icons, there is no authentication procedure performed to see if the user may run the service.

Third, it is noted that it is the browser of Raduchel which receives and sends the authentication information to the authentication manager. In essence, the browser is little more than a log-on prompt/dialog box. The PIN is not hidden from the browser. Further, the authentication being performed is not for the purpose of determining whether the user may run the browser. The browser is already running and being used by the user. In addition, claim 1 recites the security manager is configured to: "give authorization to run said application if the PIN code of the user matches the registered PIN code." Again, as recited in claim 1 it is the application which presents the PIN entry field and provides the request for user authentication which is potentially given authorization to run. In contrast, as already discussed, the authentication performed in Raduchel does not give authorization to run the browser. Raduchel simply discloses an entirely different system than that claimed.

Accordingly, there is no direct relationship between an application and authorization to run the application as recited. The claims recite a direct relationship between a particular application and authorization to run the particular application. Further, the request for user authentication is supplied "from the application" (i.e., the application the user desire to run). Finally, the authorization signal is then given "to said application" to "run said application." These features are not disclosed by Raduchel or Patterson.

For at least the above reasons, Applicant submits neither the disclosed browser nor services of Raduchel are equivalent to the application as recited and not all of the features of claim 1 are disclosed by the cited art, either singly or in combination. For at least these reasons, claim 1, and each of the independent claims, are patentably distinguishable from the cited art and a prima facie case of obviousness is not established.

In addition to the above, the cited art does not disclose a security manager configured to "supply information to the application about PIN code entering key-pressing operations by the user, wherein the entered PIN code is not supplied to the application." First, as discussed above, Raduchel does not disclose the security manager supplying information to "said" application as recited. Rather, Raduchel discloses returning a permissions type token to the browser. Second, Raduchel includes no teaching or suggestion of a security manager supplying information concerning PIN code key-pressing operations to the application without the PIN code being supplied to the application. These features are nowhere found in the cited art. It is suggested by the examiner that these features are disclosed by Raduchel in the following:

> "The authentication manager receives the log-in information and uses it to authenticate the user, as shown in FIG. 4. Although various embodiments of the authentication manager may vary and could be configurable, in one implementation, the authentication manager receives a log-in request containing a user name and password (step 402 in FIG. 4). After receiving this information, the authentication manager authenticates the user by accessing the authentication file to determine if the user name and password are contained in it (step 404) and returns a token that identifies the services that the user may use (step 406). Additionally, this token may contain a profile of the user's access rights, and when the token is returned to the local computer, it would be included in all further requests from the local computer. Returning to FIG. 2, the local computer receives the authentication results from the authentication manager and determines if the user was authenticated (step 208)." (Raduchel, col. 5, lines 17-34).

Clearly, the above disclosure does not describe a security manager supplying information concerning key-pressing operations to the application. Rather, the remote authentication manager receives the complete authentication information from the local computer, performs an authentication check, and returns a result (profile, access rights) to the local computer. Further, there is no disclosure of providing the recited key-pressing information without providing the PIN code. Therefore, for at least these additional reasons, each of the independent claims are patentably distinct from the cited art. Finally, as each of the dependent claims includes the features of the independent claims upon which they depend, the dependent claim are patentable for at least the reasons given above.

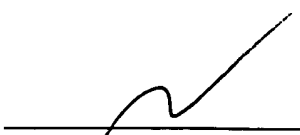
In addition to the above, Applicant notes that neither claim 5 nor claim 6 were addressed by the examiner.

In light of the foregoing remarks, Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicant hereby petitions for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5266-09100/RDR.

Also enclosed herewith are the following items:

☒ Return Receipt Postcard
☒ Notice of Appeal
☒ Petition for Extension of Time
☒ Fee Authorization

Respectfully submitted,



Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: September 11, 2006